Silverfort

Silverfort Alignment with The ACSC Essential Eight Maturity Model – Protect your Identity Attack Surface

WHITE PAPER

Foreword

This document specifies how organisations can use the Silverfort Unified Identity Protection platform to implement the identity protection aspect of the Essential Eight Maturity Model framework per its recent update in October 2021. Silverfort addresses two groups of mitigation strategies that focus on restricting admin privilege and enforcement of multi-factor authentication. Silverfort also provides additional advanced capabilities within these two groups, that while being beyond the scope of the Essential Eight Maturity Model, are nevertheless imperative for sound protection against today's threat landscape. Security stakeholders that rely on the Essential Eight as a guideline can learn how Silverfort could partner with them in their journey towards a more resilient security posture following the framework, as well as gain insights into key attack surfaces that Silverfort is uniquely positioned to address, such as lateral movement and ransomware propagation.

How to use this document?

The document is divided into three parts:

1. Overview

The Essential Eight objective, what mitigation strategies Silverfort covers, and what actual protections these strategies translate to when implemented.

2. Silverfort Essential Eight Mapping

A table that lists the various strategies Silverfort checks within the 'restrict administrative access' and 'multi-factor authentication' groups.

3. From compliance to protection

A detailed explanation of the protection Silverfort delivers to three key attack surfaces that don't have corresponding Essential Eight mitigation strategies.

Part 1: Overview

What is The Essential Eight Maturity Model?

The Essential Eight was developed by the Australian Cyber Security Centre (ACSC) as a prioritized mitigation strategy, aimed to assist Australian businesses in the design and building of their protections against today's cyberattacks. Initially designed for Microsoft Windows-based internet-connected networks, the framework focuses on reducing the attack surface of these environments across various attack stages. The Essential Eight defines three targeted maturity levels that differ from each other by the respective level of potential threat actors, from basic attacks that utilize commoditized hacking tools to sophisticated tailor-made operations that employ highly skilled attacks on specific targets.

1. Application control

2. Patch applications

3. Configure Microsoft Office macro settings

4. User application hardening

5. Restrict administrative privileges

6. Patch operating systems

7. Multi-factor authentication

8. Regular backups

What Parts of the essential Eight Does Silverfort Address?

The Silverfort Unified Identity Protection platform assists organisations in complying with two sets of mitigation strategies:

- **Restrict administrative privileges**

While it is clear that these controls were written with a Privileged Access Management (PAM) solution in mind, Silverfort can address those that are related to runtime access control (see the part 2 below for further details). Organisations that acknowledge the importance of these controls but are struggling with their PAM implementation should consider Silverfort as a complimentary, rapid-time-to-value solution for these controls.

- **Multi-factor authentication**

Silverfort fully addresses all of the required controls across the three maturity levels outlined in the Essential Eight framework. Moreover, there are some specific controls that Silverfort alone can provide, such as MFA and adaptive access for legacy applications and administrative command-line interfaces. Organisations that have prioritized this control in their security architecture road map can rely on Silverfort to check all the required boxes.

WHAT PROTECTION DO THESE MITIGATIONS PROVIDE?

The objective of both the **'restrict administrative privileges'** and **'multi-factor authentication'** mitigation strategies is to prevent the spread of an attack that has gained an initial foothold in the targeted environment. The prominent example is an attacker who has managed to gain remote control on an employee's machine or an internet-facing server. The attacker's next step would be to expand their presence in the environment bycompromising user credentials - preferably administrative ones – and using them to log in to additional machines.

Restriction of administrative privileges aims to place hurdles in the attacker's ability to utilize compromised admin credentials for malicious access, while MFA serves as an additional protection layer to ensure that even if the credentials used are valid, they cannot be used to access any resource without the explicit verification of the legitimate user.

Part 2: Silverfort Essential Eight Mapping

Maturity Level 1

Objective

The following is an excerpt from Essential Eight. The parts that correspond to 'restrict administrative privileges' and 'multi-factor authentication' are bolded:

"The focus of this maturity level is adversaries who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, systems. For example, adversaries opportunistically use a publicly-available exploit for a security vulnerability in an internet-facing service that had not been patched or authenticating to an internet-facing service using credentials that were stolen, reused, brute-forced or guessed. Generally, adversaries are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Adversaries will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications, for example via Microsoft Office macros. ***If the account that an adversary compromise has special privileges they will seek to exploit it****. Depending on their intent, adversaries may also destroy data (including backups)."*

Compliance Table

Restrict administrative privileges

Mitigation Strategy	Silverfort Protection
Requests for privileged access to systems and applications are validated when first requested.	
Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	
Privileged users use separate privileged and unprivileged operating environments.	
Unprivileged accounts cannot log on to privileged operating environments.	
Privileged accounts (excluding local administrator accounts) cannot log on to unprivileged operating environments.	🛡

Mitigation Strategy	Silverfort Protection
Multi-factor authentication is used by an organisation's users if they authenticate to their organization's internet-facing services.	🛡
Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	🛡
Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	🛡
Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	🛡

Maturity Level 2

Objective

The following is an excerpt from the Essential Eight. The parts that correspond to 'restrict administrative privileges' and 'multi-factor authentication' are bolded:

"The focus of this maturity level is adversaries operating with a modest step-up in capability from the previous maturity level. These adversaries are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these adversaries will likely employ well-known tradecraft in order to better attempt to bypass security controls implemented by a target and evade detection.

This includes ***actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication****. Generally, adversaries are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Adversaries will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications, for example via Microsoft Office macros.* ***If the account that an adversary compromises has special privileges they will seek to exploit it, otherwise they will seek accounts with special privileges****. Depending on their intent, adversaries may also destroy all data (including backups) accessible to an account with special privileges."*

Compliance Table

Restrict administrative privileges

Mitigation Strategy	Silverfort Protection
Requests for privileged access to systems and applications are validated when first requested.	
Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	
Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	
Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	
Privileged users use separate privileged and unprivileged operating environments.	
Privileged operating environments are not virtualised within unprivileged operating environments.	
Unprivileged accounts cannot log on to privileged operating environments.	🛡
Privileged accounts (excluding local administrator accounts) cannot log on to unprivileged operating environments.	🛡
Administrative activities are conducted through jump servers.	🛡
Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.	
Use of privileged access is logged.	🛡
Changes to privileged accounts and groups are logged.	
Requests for privileged access to systems and applications are validated when first requested.	

Compliance Table

Multi-factor authentication

Mitigation Strategy	Silverfort Protection
Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	🛡
Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	🛡
Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	🛡
Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	🛡
Multi-factor authentication is used to authenticate privileged users of systems.	🛡
Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	🛡
Successful and unsuccessful multi-factor authentications are centrally logged.	🛡

Maturity Level 3

Objective

The following is an excerpt from the Essential Eight. The parts that corresponds to 'restrict administrative privileges' and 'multi-factor authentication' are bolded:

"The focus of this maturity level is adversaries who are more adaptive and much less reliant on public tools and techniques. These adversaries are able to exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older software or ***inadequate logging and monitoring****. Adversaries do this to not only extend their access once initial access has been gained to a target, but to* ***evade detection and solidify their presence****. Adversaries make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.*

Generally, adversaries may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical security controls implemented by their targets. For example, this includes social engineering a user to not only open a document but also to unknowingly assist in bypassing security controls. This can also include ***circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user****. Once a foothold is gained on a system,* ***adversaries will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks****. Depending on their intent, adversaries may also destroy all data (including backups)."*

Compliance Table

Restrict administrative privileges

Mitigation Strategy	Silverfort Protection
Requests for privileged access to systems and applications are validated when first requested.	
Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	
Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	
Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.	
Privileged accounts are prevented from accessing the internet, email and web services.	
Privileged users use separate privileged and unprivileged operating environments.	
Privileged operating environments are not virtualised within unprivileged operating environments.	
Unprivileged accounts cannot logon to privileged operating environments.	🛡
Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	🛡
Just-in-time administration is used for administering systems and applications.	
Administrative activities are conducted through jump servers.	🛡
Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.	
Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.	
Use of privileged access is centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	🛡
Changes to privileged accounts and groups are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	

Compliance Table

Multi-factor authentication

Mitigation Strategy	Silverfort Protection
Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	🛡
Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	🛡
Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	🛡
Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	🛡
Multi-factor authentication is used to authenticate privileged users of systems.	🛡
Multi-factor authentication is used to authenticate users accessing important data repositories.	🛡
Multi-factor authentication is verifier impersonation resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	🛡
Successful and unsuccessful multi-factor authentications are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	🛡

Part 3: From Compliance to Actual Protection – The Silverfort Difference

The Essential Eight framework is a means rather than an end by itself and is meant to assist organisations in increasing their resilience to cyberattacks. To support this purpose, this section highlights three places where implementation of the framework requirements alone leaves unaddressed security gaps, and describes how the Silverfort platform addresses these gaps to ensure your environment is fully protected.

360° Protection Against Lateral Movement and Ransomware Propagation

While any standard MFA solution suffices to checkbox the three maturity levels of the respective Essential Eight controls, **Silverfort is the only solution that provides proactive prevention of lateral movement and ransomware propagation by extending MFA protection across all access interfaces in the on-prem environment.**

There are many ways to conduct remote access between machines within the enterprise perimeter. Common MFA solutions typically address access via Remote Desktop Access (RDP), to prevent attackers from utilizing it for malicious access. However, this is not enough since most attacks make use of command line tools such as PsExec, Remote PowerShell, WMI and others which are beyond the scope of these solutions. So, while the Essential Eight MFA controls don't specify the coverage of these access interfaces as a requirement, their inclusion in the MFA scope is imperative to achieve the goals this framework has set.

Silverfort utilizes an innovative, agentless technology to enforce MFA across all protocols and access interfaces within the protected environment. In this manner, any connection the attacker attempts to perform from the initially compromised machine to others in the environment encounters an MFA barrier – regardless of what access interface was used.

Native Risk Engine for Adaptive Access Policies

Another key capability that is not listed in the Essential Eight framework is to base the MFA policies on risk analysis. In practice, MFA solutions that rely exclusively on preset rules encounter significant challenges in balancing protection needs with user experience and minimizing work disruption. Silverfort's risk engine supports adaptive access policies that can be triggered by either an overall risk score or even specific risk indicators (brute force, lateral movement, etc.). In that manner, users are prompted with MFA only when actual risk is detected.

Service Account Protection

The Essential Eight framework explicitly excludes service accounts from the scope of restrict privileged access controls, because these controls were apparently defined based on PAM solutions password rotation capabilities. However, it's important to acknowledge that service accounts are considered a prime target for attackers and are utilized extensively for lateral movement and ransomware propagation. Silverfort goes beyond the Essential Eight requirements to provide comprehensive service accounts protection suite with automated discovery, monitoring, risk analysis and policy creation for all service accounts within the protected environment.

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver end-to-end identity security across the entire IAM infrastructure, eliminating gaps and blind spots, giving businesses visibility into their identity fabric and extending protection to resources that previously could not be protected. This is all done via a patented technology that natively integrates with your entire IAM infrastructure, Runtime Access Protection™ (RAP). It is lightweight, easy to use and deploy, and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline to stop lateral movement, ransomware propagation, and other identity threats.

To learn more, visit www.silverfort.com